IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim- Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

DEFENDANTS' JOINT OPPOSITION TO SRI INTERNATIONAL, INC.'S MOTION FOR PARTIAL SUMMARY JUDGMENT OF NO ANTICIPATION BY THE "EMERALD 1997" PUBLICATION

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree St.
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5100

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS, JAMES, HITCHENS
& WILLIAMS, LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel: (302) 888-6800
Fax: (302) 571-1750

OF COUNSEL:
Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
DAY CASEBEER MADRID
& BATCHELDER LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

Dated: June 30, 2006

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

I. INTRODUCTION

More than one year before the filing date of the patents-in-suit, one of the named inventors published an article – EMERALD 1997 – describing the alleged inventions described and claimed in the patents-in-suit. There is no dispute that the article is prior art. Nor is there any dispute that figures and substantial portions of the text of EMERALD 1997 were simply copied verbatim into the specification of the patents-in-suit. Nor is it disputed that the inventors and SRI's own expert have conceded that EMERALD 1997 describes most, if not all, of the elements of the claims of the patents-in-suit. Accordingly, Defendants have moved for summary judgment of invalidity based on EMERALD 1997 with respect to the asserted claims of the '212, '203, and '615 patents.

Faced with these undisputed facts, SRI seeks to forestall summary judgment of invalidity by filing its own motion for partial summary judgment of no anticipation based on EMERALD 1997. But SRI fails to address the '212 patent. SRI's silence is understandable in light of the fact that one of the inventors admitted at his deposition that EMERALD 1997 described all of the limitations of claim 1 of the '212 patent.[1] Through its silence, SRI implicitly concedes that the '212 patent claims are anticipated by EMERALD 1997.

With respect to the '203, '615, and '338 patents, the sole basis for SRI's motion is its contention that EMERALD 1997 does not describe expressly or inherently any one of the network traffic data categories recited in some of the claims-in-suit. Rather than address Defendants' actual positions, however, SRI attempts to rewrite the EMERALD 1997 paper to exclude key disclosures. SRI also seeks to impose an inherency standard

---

[1] Valdes Tr. at 466-67 [D.I. 301, Ex. U].

unsupported in law that would effectively make the doctrine impossible to meet. SRI argues that to be inherent the disclosure must automatically or necessarily lead one of skill to actually construct the specific embodiment. Under the law, however, inherency is met when the prior art reference describes and enables an embodiment which necessarily includes the claimed subject matter.

This correct standard is met here. Contrary to SRI's arguments, a reasonable jury could only conclude that EMERALD 1997 discloses and enables an embodiment of a network monitoring system that necessarily uses at least one of the recited network traffic data categories. EMERALD 1997 discloses the use of firewalls as a data source for network packets. The data provided by firewalls existing at the relevant time necessarily included data corresponding to some of the recited categories in the claims. This was not "an unguided complex design choice," as SRI alleges, it was an express teaching of EMERALD 1997. EMERALD 1997 thus expressly or inherently discloses the recited network traffic data categories.

Based upon this evidence, summary judgment of ***invalidity*** is appropriate. At the very least, SRI has failed to prove there is no genuine issue of a material fact regarding whether EMERALD 1997 inherently discloses to one of ordinary skill in the art the recited network traffic data categories. SRI's motion for summary adjudication of no anticipation based on EMERALD 1997 should therefore be denied.

II. SRI'S MOTION FOR PARTIAL SUMMARY JUDGMENT OF NO INHERENT ANTICIPATION BY EMERALD 1997 SHOULD BE DENIED

A. Legal Standard

For summary judgment to be entered in its favor, SRI must prove that "no genuine issue exists as to any material fact" and that it "is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). As SRI concedes, a prior art reference may anticipate

without expressly disclosing a particular limitation if that limitation is inherently present in the reference. *See Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d 1550, 1554 (Fed. Cir. 1995). As SRI also admits, the relevant inquiry is whether the prior art sufficiently describes and enables at least one embodiment which necessarily includes the subject matter embraced by the particular claim limitation. *See Toro Co. v. Deer & Co.*, 355 F.3d 1313, 1321 (Fed. Cir. 2004); *see also Continental Can Co. USA, Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991). Whether a prior art reference inherently describes a claimed limitation to one of ordinary skill in the art is a question of fact. *See In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997).

Defendants need not show, as SRI contends, that a person of ordinary skill in the art reading EMERALD 1997 would "necessarily construct" a system which analyzed the recited network traffic data categories.[2] As the Federal Circuit has explained, the focus is on what the reference ***discloses***: "The dispositive question regarding anticipation is whether one skilled in the art would reasonably understand or infer from the prior art reference's teaching that every claim [limitation] was disclosed in that single reference." *See Akamai Techs. v. Cable & Wireless Internet Servs.*, 344 F.3d 1186, 1192 (Fed. Cir. 2003) (internal quotations omitted).

SRI argues that Defendants bear a heavier burden here because EMERALD 1997 was before the Patent Examiner during prosecution. However, the Federal Circuit has recognized that there are references previously considered by an Examiner which contain "disclosure so poignantly impacting upon patentability as to render virtually irrelevant the fact of its consideration by the examiner." *Lear Siegler, Inc. v. Aeroquip Corp.*, 733

---

[2] SRI International, Inc.'s Opening Brief in Support of its Motion for Partial Summary Judgment of No Anticipation by the "EMERALD 1997" Publication ("Opening Br.") at 7 [D.I. 277].

F.2d 881, 886 n.4 (Fed. Cir. 1984). Given the closeness of the disclosures of EMERALD 1997 to the claims of the patents-in-suit, the overlap in authorship, and the Examiner's silence on all prior art issues during prosecution, EMERALD 1997 is just such a reference.

B. SRI is Not Entitled to Judgment as Matter of Law Because EMERALD 1997 Inherently Discloses Recited Network Traffic Data Categories to Person of Ordinary Skill in the Art.

As set forth in Defendants' Opening Brief in Support of Their Motion for Summary Judgment, EMERALD 1997 sufficiently describes and enables an embodiment of monitoring network packet data at a firewall that necessarily would monitor one or more of the recited network traffic categories.

SRI attempts to rewrite the EMERALD 1997 article in arguing against inherency. Rather than describe the actual data sources EMERALD 1997 discloses, SRI contends the paper only mentions the possibility. Thus, SRI improperly reduces Defendants' anticipation defense to:

> (1) EMERALD 1997 discloses monitoring a network by selection of a target specific even stream, which *might* be derived from an application log; (2) the application log *might* be a firewall log; (3) [*some*] firewalls known in 1997 *might be configured* to monitor packet data volume or network connection requests and denials; therefore (4) EMERALD 1997 allegedly *necessarily* discloses monitoring and analyzing packet data volume and network connection requests and denials.[3]

SRI's self-serving characterization, however, does not accurately reflect Defendants' position and ignores several key explicit disclosures in EMERALD 1997.

The teaching of EMERALD 1997 is far more explicit than SRI claims. EMERALD 1997 directly teaches monitoring network traffic at firewalls. At the beginning of EMERALD 1997, the authors explained that one of the problems that they

---

[3] Opening Br. at 4 (citations omitted) [D.I. 277].

were trying to solve was how to extend techniques that had been developed to monitor centralized computing resources to "cover spatially distributed components such as network ***infrastructure*** (e.g., routers, filters, DNS, ***firewalls***)."[4] The authors of EMERALD 1997 then described that their solution involved deploying monitors to directly analyze such infrastructure: "Service monitors are dynamically deployed within a domain to provide localized real-time analysis of ***infrastructure*** (e.g., routers or gateways) . . . ."[5] EMERALD 1997 then went on to explain that the data or events the monitors would analyze could be "derived from a variety of sources including audit data, ***network datagrams***, SNMP traffic, application logs, and analysis results from other intrusion-detection instrumentation."[6] Thus, one of ordinary skill in the art would have understood EMERALD 1997 to ***expressly*** teach monitoring of network datagrams (i.e., network packets) received at firewalls (i.e., infrastructure).[7]

While it is true that EMERALD 1997 does not expressly describe a particular example of a network traffic data category like network connection requests and network connection denials, there is no ***genuine*** dispute that one of ordinary skill in the art would have understood the description of monitoring network datagrams at firewalls to necessarily include monitoring network connection requests and network connection denials. The reason is simple. A firewall monitors and screens network traffic, letting

---

4 EMERALD 1997 at 354 [D.I. 301, Ex. E].

5 EMERALD 1997 at 355 [D.I. 301, Ex. E].

6 EMERALD 1997 at 356 [D.I. 301, Ex. E].

7 SRI's own expert and one of the named inventors have admitted that the term network datagram is equivalent to a network packet. Kesidis Tr. at 670-72 [D.I. 301, Ex. V]; Porras Tr. at 416-19 [Declaration of Robert G. Galvin in Support of Defendants' Joint Opposition to SRI International, Inc.'s Motion for Partial Summary Judgment of No Anticipation by the "Emerald 1997" Publication ("Galvin Decl.") Ex. A].

some packets in and keeping some packets out.[8] When configuring a firewall, one must necessarily define what kinds of data pass through and what kinds of data are blocked. As the authors of one of the leading guides for Internet security explained in 1996, "To set up your firewall, you must therefore define what kinds of data pass and what kinds are blocked."[9]

In other words, a firewall ***necessarily*** monitored passed though traffic and discarded traffic. If it did not monitor network traffic data to allow certain packets and block others, it was not a firewall. Packets that a firewall did not allow into the network because they violated certain rules were, by definition, network connection denials.[10] Thus, even if a firewall did not generate a log that could be later reviewed, it still inherently monitored network traffic and, as the EMERALD 1997 paper disclosed, could act as a data source for EMERALD network monitors. Thus, in this disclosed embodiment, EMERALD monitors that generated reports of suspicious activity as a result of the firewall activity, would necessarily base their analysis on network traffic data from firewalls concerning network packets that were passed through or blocked. Thus, the claim limitations that recited analysis based on these categories were inherently met by this disclosed embodiment. SRI therefore cannot establish it is entitled to judgment in its favor.

The fact that firewalls in 1997 routinely logged for review allowed packets or

---

[8] Avolio Decl. ¶ 60 [D.I. 301, Ex. X]; *see also Computer Dictionary* (Microsoft Press 3d ed. 1997) at 197 [D.I. 301, Ex. LL].

[9] S. Garfinkel & G. Spafford, PRACTICAL UNIX & INTERNET SECURITY (1996) at 638 [D.I. 301, Ex. AA].

[10] Kesidis Tr. at 688-89 [D.I. 301, Ex. V]; *see also* Porras Tr. at 378-79 [Galvin Decl. Ex. A]. The patent specification contemplates monitoring event streams derived from "discarded traffic (i.e., packets not allowed through the gateway because they violate filtering rules)." *See* '338 col. 5:4-7 [D.I. 301, Ex. A].

blocked packets provides further support, but is not essential to, Defendants' anticipation defense.[11] A standard firewall in 1997 also monitored and logged the amount of packet data sent over each particular connection (i.e., "network packet data volume").[12] While SRI alleges that "the logging capabilities of firewalls varied considerably" and that "[s]ome firewalls did not even have logging capabilities,"[13] it does not point to a single firewall that did ***not*** have the capability to log allowed or blocked packets. The only "evidence" that SRI cites is a misleading snippet from the deposition of Symantec's expert, Fred Avolio, which it argues establishes that "'certainly not all' firewalls that existed in 1998 had logging capability."[14] Contrary to SRI's characterization, Mr. Avolio's complete answer makes clear that one of ordinary skill in the art would have understood a firewall to have logging capabilities:

> Q. Would you agree that as of 1998, that some firewalls did not have logging capabilities?
>
> . . .
>
> THE WITNESS: All firewalls that – well, some value of "all." ***All the major firewalls at the time did some logging. It was a requirement of any security system to have logging***.
>
> In fact, most of the firewalls at the time – most of the firewalls at the time routinely and somewhat automatically did logging, in that most of them were built on some version of Berkeley UNIX using the syslog utility. It was a standard utility for years before that time period. It was just something that software developers used when developing software on UNIX systems. It was also something that was standard on firewalls. ***It was a requirement to have logging on a firewall.***
>
> BY MR. POLLACK:

---

[11] Avolio Decl. ¶¶ 61-71 [D.I. 301, Ex. X]; D.B. Chapman & E. Zwicky, BUILDING INTERNET FIREWALLS (1995) at 179-80, 400 [D.I. 301, Ex. DD]; Porras Tr. at 295 [D.I. 301, Ex. T].

[12] Avolio Decl. ¶¶ 72-78 [D.I. 301, Ex. X]; *see also* S. Garfinkel & G. Spafford, *supra*, at 639 [D.I. 301, Ex. AA].

[13] Opening Br. at 8 [D.I. 277].

[14] *Id.* [D.I. 277].

> Q. So would it be your opinion that all firewalls that existed in 1998 all had logging capability?
>
> MS. BROWN: Objection; vague, calls for speculation.
>
> THE WITNESS: Certainly not all, because "all firewalls" include the simplest router. Today the simplest firewalls, on home systems, for example, or on a Windows PC or on a Macintosh, do some kind of logging. All do. I'm sure there – ***I shouldn't say I'm sure. I suppose there might have been firewalls that did not do logging. But that was a requirement of -- of -- of firewalls at the time.***[15]

In fact, SRI's own expert, Dr. Kesidis, agreed with Mr. Avolio. During his deposition, Dr. Kesidis admitted that in 1997 a firewall "would inform me typically of what packets it blocked" and that "you could configure them to record what they blocked."[16] Thus, the evidence of record overwhelmingly supports Defendants' contention that one of ordinary skill in the art would have understood EMERALD 1997's reference to monitoring network traffic at a firewall to necessarily include the capability of generating a log based upon monitoring at least one of (a) network connection requests, (b) network connection denials, or (c) network packet data volume. For these reasons, Defendants contend that they, not SRI, are entitled to judgment as a matter of law.

SRI's motion also challenges several arguments raised in Defendants' expert reports.[17] Defendants' experts have offered opinions that it would have been inherent to select at least one of the recited network traffic data categories based solely upon EMERALD 1997's teaching to monitor network datagrams (i.e., network packets) for

---

15 Avolio Tr. at 42-43 [D.I. 278, Ex. M].

16 Kesidis Tr. at 688-89 [D.I. 301, Ex. V].

17 Defendants did not rely on these positions in their motion for summary judgment to avoid complicating the motion, since the disclosure relating to using firewalls as the data source for network traffic information is so clear. Inherency based on the disclosure of "network datagrams" is an alternative argument that is supported by the evidence,

intrusive activity. In Stephen Smaha's opinion, "Inherent in the use of these network packet capture and analysis routines are the examination of network packet data transfer commands, volumes, errors, requests, and denials."[18] Or, as Todd Heberlein explained, given the known types of intrusive attacks, one of ordinary skill in the art would have necessarily monitored one or more of the recited network traffic data categories.[19]

For example, throughout the 1990s, the Computer Emergency Readiness Team ("CERT") regularly issued public advisories warning of new types of attacks. In September 1996, CERT first issued a warning about SYN flooding and IP Spoofing attacks.[20] As the advisory explained, a SYN flooding attack involves sending numerous requests to open a network connection that cannot be responded to, flooding the system with half-open connections and making it difficult for the system to continue to communicate.[21] One of ordinary skill in the art would have been familiar with attacks like SYN flooding, and therefore understood that if you were monitoring network traffic data, you should monitor categories like network connection requests and denials.[22] In other words, just as the disclosure of a burglar alarm to prevent entry into a house would necessarily teach one of ordinary skill in the art to monitor doors and windows, the disclosure of a network intrusion detection system would necessarily disclose monitoring standard network traffic categories like network connection denials or network packet data volumes.

---

which also establishes that SRI's motion for summary judgment is inappropriate.

18 Expert Report of Stephen E. Smaha at 31 [D.I. 278, Ex. J].

19 Heberlein Decl. ¶¶ 53-58 [D.I. 301, Ex. Y].

20 CERT Advisory CA-1996-21 [SYM_P_0548726-734] [Galvin Decl. Ex. C].

21 *Id.*; *see also* Heberlein Decl. ¶ 57 [D.I. 301, Ex. Y].

22 Heberlein Decl. ¶ 57 [D.I. 301, Ex. Y].

SRI attempts to dismiss these arguments on the grounds that the "mere possibility" that one of ordinary skill in the art would have selected to monitor the recited network traffic data categories "cannot as a matter of law support a conclusion that such subject matter is inherently disclosed in EMERALD 1997."[23] But Defendants do not contend that the selection to monitor at least one of these recited categories was a mere possibility. Defendants contend it was an inevitability.

Monitoring the recited network traffic data categories was not new or novel. The inventors acknowledged that others had monitored many of the claimed network traffic data categories before them.[24] For example, during his deposition, Mr. Porras admitted:

> Q. Didn't people, prior to your work in the patent, monitor data transfers in a network?
>
> A. Yes, I think there were situations where people would do that, yes.
>
> Q. Were you and Mr. Valdes the first to describe in your patents monitoring a network for errors?
>
> A. I do not think we were the first.
>
> . . . .
>
> Q. . . . My question was simply do you believe that you and Mr. Valdes were the first to monitor a network for network packet data volume. No one else had measured that before you?
>
> A. Oh, okay. I'm sorry. I thought you asked another question where you asked me to clarify, and I was clarifying.
>
> So back to your question, I don't think we necessarily were. I don't think we are.
>
> . . . .
>
> Q. Were you and Mr. Valdes the first to invent monitoring a network for network connection requests?

---

23 Opening Br. at 11 [D.I. 277].

24 Porras Tr. at 289-95, 444-54 [D.I. 301, Ex. T]; Valdes Tr. at 283-87 [D.I. 301, Ex. U].

A. I don't think so.

Q. And were you and Mr. Valdes the first to invent monitoring a network for network connection denials?

A. I don't think we were.[25]

Nor were the network traffic data categories listed in the claims a small subset of network traffic categories that could potentially be selected; they broadly encompass most, if not all, network traffic.[26] The tools to monitor network packets that were available in 1997, such as network packet sniffers, necessarily monitored one or more of the recited network traffic data categories.[27] Given these facts, Defendants' evidence supports more than just a finding of a "mere possibility" that one of ordinary skill in the art would have understood EMERALD 1997 to disclose the recited network traffic data categories. SRI's motion should therefore be denied.[28]

C. At a Minimum, Defendants Have Submitted Evidence Sufficient to Give Rise to Genuine Issue of Material Fact Regarding the Inherent Disclosure of EMERALD 1997

If the Court declines to enter summary judgment of invalidity in Defendants' favor, Defendants have at least submitted evidence sufficient to give rise to a genuine issue of material fact that would preclude granting partial summary judgment of no anticipation based on EMERALD 1997. As noted above, whether a reference inherently

---

25 Porras Tr. at 289-94 [D.I. 301, Ex. T].

26 Valdes Tr. at 448-49 [Galvin Decl. Ex. B]; Porras Tr. at 359-61 [Galvin Decl. Ex. A].

27 Expert Report of Stephen E. Smaha at 30-31 [D.I. 278, Ex. J].

28 It should be noted that even if the Court were to find that EMERALD 1997 did not inherently disclose the recited network traffic data categories of the asserted claims of the '203 and '615 patents, Defendants' motion for summary judgment establishes that those claims are nevertheless invalid for obviousness, given the explicit suggestion to combine EMERALD 1997 with certain cited references. *See* Defendants' Brief in Support of Joint Motion for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§

discloses a claim limitation is a question of fact.[29] The evidence establishes that EMERALD 1997 discloses firewalls as a data source to monitor. While Defendants believe it is beyond genuine dispute that one of ordinary skill in the art would have understood that firewalls existing as of the time of the publication would have necessarily provided network data corresponding to at least one of the categories recited in the claims, there is, at a minimum, a genuine issue of material fact precluding summary judgment.[30] In addition, Defendants have presented evidence establishing that EMERALD 1997's disclosure of the use of network datagrams would have necessarily disclosed to one of ordinary skill in the art at least one of the recited network traffic categories.[31] Again, at a minimum, there is a genuine issue of material fact precluding summary judgment. SRI's motion for partial summary judgment of no anticipation by EMERALD 1997 should therefore be denied.

---

102 and 103 at 30-32 [D.I. 299].

29 *See In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997).

30 *See* Kesidis Tr. at 688-89 [D.I. 301, Ex. V]; Avolio Decl. ¶¶ 60-78 [D.I. 301, Ex. X]; Porras Tr. at 295 [D.I. 301, Ex. T]; S. Garfinkel & G. Spafford, PRACTICAL UNIX & INTERNET SECURITY (1996) at 638 [D.I. 301, Ex. AA]; D.B. Chapman & F. Zwicky, BUILDING INTERNET FIREWALLS (1995) at 179-80, 400 [D.I. 301, Ex. DD].

31 *See* Porras Tr. at 289-95, 444-54 [D.I. 301, Ex. T]; Valdes Tr. at 448-49 [Galvin Decl. Ex. B]; Expert Report of Stephen E. Smaha at 30-31 [D.I. 278, Ex. J]; CERT Advisory CA-1996-21 [SYM_P_0548726-734] [Galvin Decl. Ex. C]; Heberlein Decl. ¶¶ 53-58 [D.I. 301, Ex. Y].

Dated: June 30, 2006

POTTER ANDERSON & CORROON LLP

/s/ Richard L. Horwitz
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree St.
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5100

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel: (302) 888-6800
Fax: (302) 571-1750

OF COUNSEL:
Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
DAY CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 30th day of June, 2006, I electronically filed the foregoing document, **DEFENDANTS' JOINT OPPOSITION TO SRI INTERNATIONAL, INC.'S MOTION FOR PARTIAL SUMMARY JUDGMENT OF NO ANTICIPATION BY THE "EMERALD 1997" PUBLICATION,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 30th day of June, 2006, the foregoing document was served via email and by Federal Express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree Street
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com

Counsel for Symantec Corporation